WHAT IS CLAIMED IS:

1. A method of managing a user's passwords for a plurality of resources using a password registry associated with said user, comprising:

(i) encrypting an unencrypted user-specified password at a process associated with said each resource;

(ii) receiving an encrypted password from said process associated with said each resource;

(iii) storing said encrypted password in said password registry, such that said unencrypted user-specified password is unknown to said password registry.

2. The method of claim 1, further comprising associating with each said encrypted password at least one piece of identifying information.

3. The method of claim 2, wherein said identifying information includes at least one of a user ID, a resource hostname, and a resource type, and the method further comprises storing said at least one of said user ID, said resource hostname and said resource type with said encrypted password.

4. The method of claim 3, further comprising utilizing at least one of said user ID, said resource hostname, and said resource type as a query key to uniquely identify said each resource and said encrypted password for said each resource.

5. The method of claim 4, further comprising:

(iv) for subsequent user access to said each resource, retrieving a corresponding one of said encrypted passwords using said query key;

(v) decrypting said retrieved encrypted password at said process associated with each resource.

6. The method of claim 5, further comprising configuring said each resource to query said password registry to determine the existence of an associated encrypted password.

7. The method of claim 6, further comprising, in the absence of an associated encrypted password, querying the user for a password and at least one piece of identifying information.

8. The method of claim 1, further comprising providing a registration mechanism for registering each resource with said password registry.

9. A method of managing a user's passwords for a plurality of password protected resources accessed from a workstation over a network, comprising:

at a workstation process associated with a network accessed password protected resource:

receiving a user selected password;

encrypting said user selected password as an encrypted password;

storing said encrypted password in a password registry.

10. The method of claim 9, further comprising:

upon a user requesting access to said network accessed password protected resource,

retrieving said encrypted password from said password registry;

at said workstation process, decrypting said encrypted password.

11. The method of claim 10, further comprising:

password controlling access to said workstation.

12. The method of claim 11 wherein said password registry is local to said workstation.

13. A computer readable medium having computer readable program code embedded in the medium for managing a user's passwords for a plurality of resources accessed from a workstation over a network, the computer readable program code including:

code for establishing a process at a workstation, said process acting as a front-end for a network accessed resource;

code for enabling said process to receive a user-specified password;

code for enabling said process to encrypt said user-specified password as an encrypted password and output said encrypted password, in association with identifying information, to a password registry;

code for enabling said process to receive a request from a workstation user to access said resource and to, in response, retrieve said encrypted password from said password registry using said identifying information.

14. The computer readable medium of claim 13, further comprising code for enabling said process to decrypt an identified encrypted password retrieved from said password registry.

15. A password registry for managing a user's passwords for a plurality of resources, comprising:

an input for receiving an unencrypted user-specified password for one of said resources;

an output for transmitting said unencrypted user-specified password to a process associated with said one of said resources for encryption at said process;

an input for receiving said encrypted password from said process;

an output to storage for storing said encrypted password.

16. The password registry of claim 15, further comprising identifying information associated and stored with each said encrypted password.

17. The password registry of claim 16, wherein said identifying information includes at least one of a user ID, a resource hostname, and a resource type.

18. The password registry of claim 17, further comprising a query key to uniquely identify said each resource and said encrypted password for said each resource, said query key utilizing at least one of said user ID, said resource hostname, and said resource type.

19. The password registry of claim 18, further comprising a decryption module for decrypting said retrieved encrypted password at said process associated with each resource.

20. The password registry of claim 19, wherein said each resource is configured to query said password registry to determine the existence of an associated encrypted password.

21. The password registry of claim 20, wherein said password registry 20 is configured to query a user for a user ID and password in the absence of an associated encrypted password.

22. A system for managing a user's passwords for a plurality of password protected resources accessed from a workstation over a network, comprising:

at a workstation process associated with a network accessed password protected resource:

means for receiving a user selected password;

means for encrypting said user selected password as an encrypted password;

means for storing said encrypted password in a password registry.

23. The system of claim 22, further comprising:

means for retrieving said encrypted password from said password registry upon a user requesting access to said network accessed password protected resource;

means for decrypting said encrypted password at said workstation process.

24. The system of claim 23, further comprising means for password controlling access to said workstation.

25. The system of claim 24, wherein said password registry is local to said workstation.